ABSTRACT OF THE DISCLOSURE

A polynomial inverse computing apparatus comprises first to sixth registers, a left shift unit, first and second exclusive-OR units, a doubling computing unit which executes doubling computation in an extension field with characteristic 2, a halving computing unit which executes halving computation in the extension field of characteristic 2, a determination unit which determines whether or not a content of each register is 0, a decrement unit which decrements the content of each register, an increment unit which increments the content of each register.